IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

IN RE: INTEL CORP. CPU MARKETING, SALES PRACTICES AND PRODUCTS LIABILITY LITIGATION This Document Relates to All Actions.	Case No. 3:18-md-2828-SI **OPINION AND ORDER**

Christopher A. Seeger, SEEGER WEISS LLP, 55 Challenger Road, Ridgefield Park, NJ 07660; Rosemary M. Rivas, GIBBS LAW GROUP LLP, 505 14th Street, Suite 1110, Oakland, CA 94612; Steve D. Larson and Jennifer S. Wagner, STOLL STOLL BERNE LOKTING & SHLACHTER PC, 209 SW Oak Street, Suite 500, Portland, OR 97204; Gayle M. Blatt, CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD LLP, 110 Laurel Street, San Diego, CA 92101; Stuart A. Davidson, ROBBINS GELLER RUDMAN & DOWD LLP, 120 East Palmetto Park Road, Suite 500 Boca Raton, FL 33432; Melissa R. Emert, STULL, STULL, & BRODY, 6 East 45th Street, New York City, NY 10017; Richard M. Hagstrom, HELLMUTH & JOHNSON PLLC, 8050 West 78th Street, Edina, MN 55439; Jennifer L. Joost, KESSLER TOPAZ MELTZER & CHECK LLP, One Sansome Street, Suite 1850, San Francisco, CA 94104; Adam J. Levitt, DICELLO LEVITT GUTZLER, Ten North Dearborn Street, 11th Floor, Chicago, IL 60602; and Charles E. Schaffer, LEVIN SEDRAN & BERMAN LLP, 510 Walnut Street, Suite 500, Philadelphia, PA 19106. Of Attorneys for Plaintiffs.

Daniel F. Katz, David S. Kurtzer-Ellenbogen, David Krinsky, and Samuel Bryant Davidoff, WILLIAMS & CONNOLLY LLP, 725 Twelfth Street NW, Washington, D.C. 20005; and Steven T. Lovett and Rachel C. Lee, STOEL RIVES LLP, 760 SW Ninth Avenue, Suite 3000, Portland, OR 97205. Of Attorneys for Defendant.

Michael H. Simon, District Judge.

In this multidistrict proceeding, Plaintiffs bring a putative nationwide class action against Defendant Intel Corporation (Intel) relating to certain security vulnerabilities in Intel's microprocessors. Plaintiffs allege that Intel knew for decades about alleged design defects in its microprocessors that created security vulnerabilities and that Intel failed to disclose or mitigate these vulnerabilities. Plaintiffs also allege that the ways in which these security vulnerabilities could be exploited became publicly known beginning in January 2018, with new ways continuing to be discovered and publicized. These forms of exploit have become generally known as "Spectre," "Meltdown," "Foreshadow," "ZombieLoad," "SwapGS," "RIDL," "LazyFP," "CacheOut," and "Vector Register Sampling," among others. Plaintiffs contend that until Intel fixes the alleged defects at the hardware level, additional ways to exploit these security vulnerabilities will likely continue to be discovered.

Plaintiffs allege that Intel's processors have two primary design defects. First, the design of the processors heightens the risk of unauthorized access to protected memory secrets. Second, the design does not completely delete, or undo, the memory's recent retrieval of those secrets, also increasing the risk of unauthorized access. Plaintiffs contend that these design defects create security vulnerabilities that could lead to a breach of confidential data. Plaintiffs also allege that Intel cannot fix these defects after-the-fact, and that the software patches created or distributed by Intel to mitigate these defects substantially diminish the speed of Intel's processors.

Intel has twice previously moved to dismiss this action. The Court granted the first motion with leave to amend. *See In re Intel Corp. CPU Mktg., Sales Pracs. & Prod. Liab. Litig.* (*Intel I*), 2020 WL 1495304 (D. Or. Mar. 27, 2020). Plaintiffs then filed an Amended Consolidated Class Action Allegation Complaint (Amended Complaint). That complaint asserted the following nationwide class claims: (1) fraud by concealment or omission; (2) breach of

California's Consumers Legal Remedies Act (CLRA), Cal. Civ. Code §§ 1750, *et seq.*; (3) breach of California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code §§ 17200, *et seq.*; (4) breach of California's False Advertising Law (FAL), Cal. Bus. & Prof. Code §§ 17500, *et seq.*; and (5) unjust enrichment, or quasi-contract. Plaintiffs also asserted separate state subclass claims for each state except California, Kentucky, and Massachusetts, plus the District of Columbia, under each jurisdiction's deceptive or unfair trade practices act or consumer protection law. Plaintiffs sought both money damages and injunctive relief.

The Court granted Intel's second motion to dismiss. *See In re Intel Corp. CPU Mktg., Sales Pracs. & Prod. Liab. Litig*. (*Intel II*), 2021 WL 1198299 (D. Or. Mar. 29, 2021). The Court gave Plaintiffs leave to amend their nationwide claim under California's UCL alleging unfair conduct, their nationwide claim for unjust enrichment, and their state subclass claims. The Court dismissed all other claims with prejudice.

Plaintiffs filed a Second Amended Consolidated Class Action Allegation Complaint (Second Amended Complaint). It asserts the two nationwide claims for which the Court granted leave to replead—breach of California's UCL for unfair conduct and unjust enrichment. It also alleges the same states' subclass claims under each jurisdiction's deceptive or unfair trade practices act or consumer protection law. Intel moves to dismiss, with prejudice, all of Plaintiffs' claims.

Against the Second Amended Complaint, Intel challenges Plaintiffs' nationwide class claims, which Intel argues under California law.[1] Intel argues that Plaintiffs' unfair conduct claim is coextensive with Plaintiffs' fraud claim under the UCL and thus should be dismissed,

[1] Intel adds that it reserves the right to argue at a later time that California law does not govern claims asserted by persons who are not residents of California.

and that Plaintiffs fail to allege a material omission or otherwise allege how Intel's conduct was unfair under the UCL. Intel also argues that Plaintiffs fail to state a claim for unjust enrichment. Intel further argues that Plaintiffs may not pursue these equitable claims because Plaintiffs have an adequate remedy at law. Finally, Intel challenges Plaintiffs' state subclass claims. Intel argues that Plaintiffs fail to state a claim for any of the six bellwether state counts that the parties agreed to litigate in the pending motion.[2] For the reasons explained below, the Court grants in part Intel's motion to dismiss the Second Amended Complaint, dismissing with prejudice all claims based on Intel's alleged conduct *before* September 1, 2017. The Court denies Intel's motion for Plaintiffs who purchased devices with Intel processors *after* September 1, 2017.

STANDARDS

A motion to dismiss for failure to state a claim may be granted only when there is no cognizable legal theory to support the claim or when the complaint lacks sufficient factual allegations to state a facially plausible claim for relief. *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010). In evaluating the sufficiency of a complaint's factual allegations, the court must accept as true all well-pleaded material facts alleged in the complaint and construe them in the light most favorable to the non-moving party. *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1140 (9th Cir. 2012); *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998 (9th Cir. 2010). To be entitled to a presumption of truth, allegations in a complaint "may not simply recite the elements of a cause of action, but must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself

[2] The parties chose Plaintiffs' claims under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA), the Illinois Consumer Fraud and Deceptive Business Practices Act (ICFA), the New Jersey Consumer Fraud Act, (NJCFA), the New York General Business Law (NYGBL), the Ohio Consumer Sales Practices Act (OCSPA), and the Texas Deceptive Trade Practices Act (TDTPA).

effectively." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). The court must draw all reasonable inferences from the factual allegations in favor of the plaintiff. *Newcal Indus. v. Ikon Off. Sol.*, 513 F.3d 1038, 1043 n.2 (9th Cir. 2008). The court need not, however, credit the plaintiff's legal conclusions couched as factual allegations. *Ashcroft v. Iqbal*, 556 U.S. 662, 678-79 (2009).

A complaint must contain sufficient factual allegations to "plausibly suggest an entitlement to relief, such that it is not unfair to require the opposing party to be subjected to the expense of discovery and continued litigation." *Starr*, 652 F.3d at 1216. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)). "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Mashiri v. Epsten Grinnell & Howell*, 845 F.3d 984, 988 (9th Cir. 2017) (quotation marks omitted).

BACKGROUND

A. General Background

Plaintiffs' Second Amended Complaint is 487 pages long and contains 1,699 separately numbered paragraphs.[3] The Second Amended Complaint contains much technical detail on the many so-called exploits (or ways in which the security vulnerabilities can be exploited) that have been discovered and become publicly known during the past four years. The Second Amended Complaint explains how these security vulnerabilities affect Intel's microprocessors, also called

[3] The Amended Complaint was 409 pages and contained 1,544 separately numbered paragraphs.

"chips" or simply "processors." It also details the history of Intel's chip development and competition with Advanced Micro Devices, Inc. (AMD). In this section, the Court summarizes the facts most relevant to the pending motion.

Intel manufactures microprocessors. A microprocessor is an integrated electronic circuit that contains the functions of a central processing unit (CPU) of a computer. The CPU is the "brains" of the computing device, performing the necessary computations for programs or applications, such as Microsoft Word, and peripheral devices, such as printers. Each program communicates with a processor through instructions, with each instruction representing a calculation or operation that the CPU must execute on behalf of the requesting program. For each calculation, the CPU "fetches" an instruction from the computer's memory, "decodes" the instruction, "executes" it, and, finally, "writes-back" the result. The time that it takes a CPU to process instructions is measured in "clock cycles." Each step in the process—fetch, decode, execute, and write-back—takes at least one clock cycle. The number of clock cycles that a CPU completes per second is known as the "clock rate." The speed of a CPU often is measured in "clock speed."

Plaintiffs allege that clock speed "is a material attribute for consumers purchasing" devices, that consumers "*really* care about speed," and that "milliseconds matter." 2d Am. Compl. ¶¶ 489, 739, 743 (emphasis in original). Intel markets its microprocessors as having faster clock speed than the processors of its competitors (including AMD) and charges a premium for its fastest processors. To obtain higher clock speed, modern processors usually implement two techniques—branch prediction and speculative execution. These techniques allow the CPU to predict what actions might be needed, perform those actions "out of order,"

and later reconcile what actions were needed versus what actions were not needed and may be discarded. The CPU then properly orders the actions that were needed.

Plaintiffs allege that Intel's design implements branch prediction, speculative execution, out-of-order execution, and an unsecured cache subsystem in a way that contains the two alleged defects. The first alleged defect (Unauthorized Access) creates windows of time during which an unauthorized user could have the processor allow unnecessary or unauthorized memory access to copies of sensitive or privileged data. *Id.*, ¶ 562. This essentially allows the return of "secrets" to a "transient instruction." *See id.*, ¶¶ 6, 677. Intel's processors, unlike its competitors' processors, returns a "read value" instead of a "dummy value" during this process. *See id.*, ¶¶ 508, 677. The second alleged defect (Incomplete Undo) allows the accessed privileged information (or data about that privileged information sufficient to allow an unauthorized user to retrieve privileged information) to remain in the CPU's cache after the mistaken or unauthorized access is discovered during the reconciliation step. *Id.*, ¶ 562.

Processors contain, among other things, an "instruction set" and "microarchitecture." The instruction set serves as an interface between a computer's software and hardware. The microarchitecture governs the various parts of the processor and how they work together to implement the instruction set. Plaintiffs describe the history of Intel's chip development, including its changes in microarchitecture and instruction sets, which the Court need not summarize here. It is enough to say that Intel designed different privilege levels in its instruction set in its 1982 processor that protect a computer's most privileged information. In 1985, Intel improved the functionality of key aspects of this design—protected mode and virtual memory. Plaintiffs allege that all modern processors use these functionalities. Plaintiffs also allege that when Intel incorporated branch prediction and speculative execution in its chips in 1995 with its

P6 architecture, Intel's chips did not return "read values" but returned a random number, the way that AMD processors worked. Plaintiffs allege that this type of processor is not vulnerable to most of the security exploits that have been recently discovered, except for Spectre.

Plaintiffs allege that in July 1999 AMD "took the 'speed crown'" for developing a faster processor than Intel. *Id.*, ¶ 490. Plaintiffs describe Intel and AMD's ongoing competition and speed "wars," and allege that Intel faced product and market difficulties for a few years. Plaintiffs allege that these problems led to Intel designing and releasing in 2006 a new chip based on a new microarchitecture that went back to its P6 microarchitecture. This new microarchitecture was called "Core." The Core chips increased the use of out-of-order execution, speculative execution, branch prediction, and cache subsystems, and boosted clock speed. According to Plaintiffs, Core, unlike P6, uses an allegedly unsafe practice of returning a "read value" instead of "dummy," or random, value, thereby creating the Intel-only Unauthorized Access defect. Thus, allege Plaintiffs, Intel made critical design choices with Core to focus on improving clock speed to the detriment of security.

Plaintiffs assert that the two alleged defects, resulting from Intel's decision to prioritize processing speed rather than security, make users' confidential information more susceptible to cache timing "side-channel attacks." Side-channel attacks are based on information gleaned from operating the computer system and are not reliant on software bugs. Plaintiffs allege that the Unauthorized Access defect has existed since 2006, and the Incomplete Undo defect has been present for at least 20 years. Plaintiffs also allege that Intel knew that its processors had increased vulnerability to cache timing side-channel attacks resulting from these two alleged design defects.

Starting in 2017, independent research teams began discovering specific processor security vulnerabilities. Plaintiffs describe these as "exploits" of the alleged defects. According to Plaintiffs, the alleged defects created the security vulnerabilities that allowed the exploits to occur. In April 2017, researchers at Google Project Zero discovered the first in a series of exploits, known as "Spectre," which comes from "speculative execution." Spectre allows for unauthorized access within the same process based on branch prediction. Spectre broadly affects processors across manufacturers. Intel was notified about Spectre by June 1, 2017.

In July 2017, researchers discovered Meltdown, an exploit that takes advantage of both Unauthorized Access and Incomplete Undo. In January 2018, a third exploit, Foreshadow, was discovered. Foreshadow also takes advantage of both Unauthorized Access and Incomplete Undo. Later in 2018, researchers discovered an exploit named "SwapGS," which was not publicly disclosed until August 2019. Plaintiffs allege that only Intel-designed chips are susceptible to SwapGS. Also in 2018, researchers began identifying a new series of exploits, categorized by Intel as "microarchitectural data sampling" or "MDS" exploits. These include RIDL (Rogue in Flight Data Load), ZombieLoad, Fallout, LazyFP, CacheOut, and Snoop-Assisted L1. These exploits have been described as "powerful" and "worrisome." The MDS exploits obtain sensitive information "in flight" versus in the cache. MDS exploits were publicly disclosed on May 15, 2019, November 12, 2019, and January 27, 2020. Plaintiffs allege that Intel embargoed information on these security vulnerabilities that affect only Intel processors for significant periods of time.

Plaintiffs assert that the discovered security exploits "take advantage" of the two alleged defects in Intel's chip design. *Id.*, ¶ 5. In January 2018, it was publicly revealed that Intel's microprocessors were vulnerable to the first of these security risks. Plaintiffs allege that the

microprocessors made by AMD and other competitors of Intel are not vulnerable to any of these alleged exploits other than Spectre. Plaintiffs also allege that other than Spectre, the exploits result from Intel's specific microprocessor design choices. Spectre, on the other hand, is a widespread vulnerability that allegedly arises from speculative execution and branch prediction, as it generally is applied in chips and is shared by other microprocessor designs.

Plaintiffs do not allege that they, or anyone else, have had their computers breached or that any data has been compromised as a result of any of the alleged defects in Intel's CPUs, through Spectre, Meltdown, Foreshadow, or any similar exploitation of the alleged defects. Plaintiffs allege, however, that the exploits have been "weaponized 'in the wild,'" already have associated malware samples, and would leave no "fingerprints" and thus would be untraceable if they had been successfully used. *Id.*, ¶¶ 12, 687, 688. Plaintiffs add that any breach that may result in the future from any of these exploits would be undetectable.

Plaintiffs also allege that Intel's mitigation efforts, including providing software patches, leave consumers more susceptible to future security breaches, caused Plaintiffs to spend time and effort researching and implementing multiple mitigation techniques, caused freezing, crashing, and other computer performance problems, and have lessened the speed or other performance features of Intel's CPUs. Plaintiffs contend that Intel has caused damage in the form of diminished value of Plaintiffs' computing devices and caused Plaintiffs to be deprived of the benefit of their bargain. Plaintiffs also assert that they would not have purchased Intel's CPUs or would not have paid as high a price as they paid if Plaintiffs had known about the alleged defects in the Intel microprocessors that created the alleged security vulnerabilities and the effects the mitigation would create.

The Second Amended Complaint adds new allegations relating to Enterprise Plaintiffs. These are small, medium, and large organizations and include businesses, governments, and educational institutions. The Enterprise Plaintiffs allege that they have unique needs relating to security, of which Intel was aware, because they are subject to federal and state laws relating to the confidential information that the Enterprise Plaintiffs maintain on their devices. The Enterprise Plaintiffs also allege that they have incurred and will continue to incur "enormous costs in mitigating and responding to" the alleged defects and the exploits, and describe the effects of mitigation unique to their situation. *Id.*, ¶ 840.

B. Public Disclosure and Intel's Knowledge

The Amended Complaint alleged Intel's knowledge of the alleged defects through technical articles, white papers, product manuals, and patent applications. In resolving the second motion to dismiss, the Court asked counsel for Plaintiffs whether the allegations in the Amended Complaint about these materials disclosed Intel's knowledge of both of the alleged defects (Unauthorized Access and Incomplete Undo). Counsel responded that "in these sections we definitely are making the allegation about the unauthorized access." ECF 202 at 11. When the Court asked about some specific articles and whether they show Intel's knowledge of one or both alleged defects, counsel explained:

> My understanding is that these articles that we cite Your Honor to are evidence of Intel's knowledge as to both defects. By relaxing—again, delaying privilege checks, allowing unauthorized access to instructions. Then allowing, once that data has been moved into the CPU subsystems, the cache and the buffers, not flushing it once speculation has gone wrong. We believe the articles support us in those respects.

Id. at 11-12. Plaintiffs alleged, however, that such highly technical information was not reasonably accessible to the public and thus did not disclose the information to the public. Am. Compl. ¶ 528.

Based on the disclosure of both defects in the technical articles, white papers, and patent applications, the Court held that Intel had not concealed either alleged defect for purposes of Plaintiffs' claims based on a material omission. *Intel II*, 2021 WL 1198299, at *7 ("Information that was known in the industry is not information that the Court finds under the facts of this case that Intel fraudulently concealed or suppressed. Nor is it information that was necessarily unavailable for the general public to discover or understand.").

In the Second Amended Complaint, Plaintiffs allege the same technical articles, white papers, product manuals, and patent applications alleged in the Amended Complaint. Plaintiffs now allege, however, that these documents "do not disclose or even discuss the Unauthorized Access Defect that is the root cause of the Intel CPU Exploits." 2d Am. Compl. ¶ 587.

DISCUSSION

A. Nationwide Claims

1. UCL Unfair Business Practice

California's UCL is written in the disjunctive and "establishes three varieties of unfair competition–acts or practices which are unlawful, or unfair, or fraudulent." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). "The statutory language referring to 'any unlawful, unfair *or* fraudulent' practice makes clear that a practice may be deemed unfair even if not specifically proscribed by some other law. . . . In other words, a practice is prohibited as 'unfair' or 'deceptive' even if not 'unlawful' and vice versa." *Id.* (emphasis in original) (citations omitted).

"[T]he proper definition of 'unfair' conduct against consumers 'is currently in flux' among California courts." *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (quoting *Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 735 (9th Cir. 2007)). The California appellate courts have articulated three tests for defining "unfair"—the "balancing

test," the "tethering test," and the test from the Federal Trade Commission Act (FTC Act). *See Drum v. San Fernando Valley Bar Ass'n*, 182 Cal. App. 4th 247, 257 (2010). As discussed in the Court's Opinion and Order resolving Intel's first Motion to Dismiss, the Court applies the balancing test. *Intel I*, 2020 WL 1495304, at *22. This test asks whether the alleged practice "violates established public policy or if it is immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1473 (2006). It requires a court to weigh the utility of the defendant's conduct against the gravity of the harm to the alleged victim. *Drum*, 182 Cal. App. 4th at 257.

Intel moves to dismiss Plaintiffs' claim for unfair conduct under the UCL, arguing that this claim is coextensive with Plaintiffs' dismissed fraud claim under the UCL, that Plaintiffs fail to identify an omission, and that Plaintiffs identify no unfair conduct without an underlying omission. Plaintiffs dispute these contentions, largely relying on Intel's alleged conduct *after* the security exploits became known in 2017.

a. Whether the Alleged Claim is Coextensive with the Dismissed UCL Fraud Claim

The Second Amended Complaint alleges in the UCL claim that: (1) Intel's CPUs contained undisclosed material defects contrary to Intel's security messaging; (2) "Intel concealed at all times relevant and never disclosed that it had implemented the Unauthorized Access Defect"; (3) in 2017, after Google Project Zero discovered Meltdown and Spectre, "Intel took a series of deliberate steps that were motivated by its goals of keeping its market share in the chip market"; (4) Intel kept the security exploits a secret longer than a normal embargo and continued to sell its products at a premium price through the time of public disclosure, even though Intel knew about its unique design defects and the mitigations that would be required; (5) Intel issued public statements that the security exploits broadly affected the industry when

Intel knew that only its processors had Unauthorized Access and were vulnerable to more exploits; (6) Intel made statements that it would put security first and fix the problem but has merely offered patches and has yet to fix the problem at the hardware level by correcting the fundamental developmental defects; (7) Intel attempted to ban users from publishing test results that show the significant negative effect of the mitigation patches; and (8) Intel manipulated the embargo period process to increase it beyond the normal 90-day period, including keeping the MDS exploits embargoed for 21 months.

Intel argues that this claim must be dismissed because it overlaps entirely with the UCL fraud claim previously dismissed with prejudice. *See Hauck v. Advanced Micro Devices, Inc.* (*Hauck I*), 2019 WL 1493356, at *15 (N.D. Cal. April 4, 2019) ("[C]ourts in this district have held that where the 'plaintiffs' unfair prong claims overlap entirely with their claims of fraud,' the plaintiffs' unfair prong claim cannot survive."), *aff'd*, 816 F. App'x 39 (9th Cir. 2020) (*Hauck II*). Plaintiffs respond that this claim is not coextensive with the dismissed fraud claim because no matter what any consumer or Intel knew about the alleged defects, it is unfair conduct under the UCL for Intel to "market itself as a company providing superior CPUs in terms of speed and performance—and in so doing exacting a premium price—but then to wash its hands when its processors deliver only middling or even *inferior* speed and performance because of measures required to address security defects in those processors." ECF 215 at 32 (emphasis in original). Thus, Plaintiffs argue, the mitigation effects have rendered Intel's conduct unfair and distinguish this claim from their fraud claim.

Based on the allegations in the Second Amended Complaint, and as argued by Plaintiffs, the only conduct alleged in support of this claim that is unrelated to the alleged omission of the Unauthorized Access defect relates to Intel's alleged conduct *after* the discovery of Spectre and

Meltdown by Google Project Zero. The Court agrees that this conduct does not entirely overlap with Plaintiffs' UCL claim based on fraud. There are other concerns, however, with basing a claim solely on post-2017 conduct. They are discussed below in section A.1.c.

b. Unfair Conduct Based on a Material Omission

Plaintiffs allege that Intel failed to disclose the Unauthorized Access defect and that this omission rendered Intel's conduct unfair under the UCL. Intel contends that this merely repackages Plaintiffs' fraud-by-omission claim under the UCL that this Court dismissed with prejudice. Intel adds that even if this conduct could support an unfair conduct claim under the UCL, the technical articles, white papers, product manuals, and patent applications, alleged in the Second Amended Complaint disclose the alleged Unauthorized Access defect, thereby eliminating any argument that Intel concealed that defect and engaged in an unfair business practice. Intel points out that Plaintiffs simply have re-alleged the identical allegations from the Amended Complaint that the Court previously found disclosed Unauthorized Access, and then Plaintiffs improperly added the allegation that these materials do not disclose that defect, contradicting Plaintiffs' previous allegations.

Plaintiffs respond first that their unfair conduct claim does not hinge on the alleged omission, relying on post-2017 conduct. Whether Intel's post-2017 conduct can support an unfair conduct claim is discussed in section A.1.c below. Plaintiffs also respond that the new allegations that Unauthorized Access was not disclosed have "clarified" their previous allegations and do not contradict or retract those allegations. The Court need not decide this dispute, however, because regardless of whether Unauthorized Defect was disclosed in the technical materials, Plaintiffs' omission-based claim fails. It fails because the Court already has dismissed Plaintiffs' fraud-based UCL claim, and Plaintiffs' assertion of an omission-based unfair conduct UCL claim is simply a UCL fraud-by-omission claim. It also fails even if it could

independently be considered a claim based on unfair conduct, because Plaintiffs fail to state such a claim.

If the technical articles, white papers, product manuals, and patent applications disclose Unauthorized Access, Intel did not conceal the material fact of this alleged defect and Intel's conduct is not unfair under the UCL because of a material omission. The allegations that purport to show *Intel's knowledge* of the alleged defects, however, are the same allegations that support the proposition that the defects were disclosed and not concealed. Thus, if the technical materials do not show public disclosure of the Unauthorized Access defect, then they also do not show Intel's knowledge of the Unauthorized Access defect. This leaves the only support for Intel's knowledge of the alleged Unauthorized Access defect the mere fact that because Intel is the manufacturer of the chips it has superior knowledge and accordingly "knew" or "should have known" about the alleged defect.

Plaintiffs allege that Intel knew that its processors were generally vulnerable to side-channel attacks, relying on the technical articles, white papers, product manuals, and patent applications. That knowledge, however, was public information. Further, as the district court and the Ninth Circuit explained in *Hauck* when addressing similar claims against AMD, knowledge of vulnerability to side-channel attacks and knowledge of the specific vulnerabilities first discovered in 2017 by Google Project Zero are not the same thing. *See Hauck II*, 816 F. App'x at 42-43; *Hauck I*, 2019 WL 1493356, at *12.

As for Intel's knowledge of the specific alleged "defects" and the resulting security vulnerabilities before Google Project Zero's discovery, Plaintiffs allege that the Unauthorized Access "defect" was an "intentional design decision by Intel," that Intel "purposely implemented the Unauthorized Access Defect to allow instructions to access the read value (instead of

returning a random number similar to Intel's P6 and AMD's CPUs)," that "the Defects were consciously designed and implemented by Intel as undisclosed performance features," and that Intel "knew (or certainly should have known) well prior to the disclosure of the Intel CPU Exploits that its defective design of its CPUs was dangerous and rendered its CPUs unsafe and insecure." 2d Am. Compl. ¶¶ 11, 508, 587. At oral argument, Plaintiffs emphasized that they are alleging that Intel violated a fundamental law of CPU design and that allegation alone is enough to allege Intel's knowledge of the defect. Plaintiffs allege that Intel "removed well-accepted hardware security and violated well-settled CPU design principles," "defied well-settled architecture design principles," and "knew that the manner in which it implemented speculative execution violated fundamental CPU design principles by removing well-accepted security to ensure memory isolation and leaving confidential information accessible to unauthorized access." *Id.*, ¶¶ 540, 562, 927. Plaintiffs also allege that Intel knew how to design its CPUs to preclude the Unauthorized Access defect (¶ 927), but this allegation is based on the patent applications, which again shows that the Unauthorized Access defect was publicly disclosed.

The Ninth Circuit has rejected general allegations of a manufacturer's knowledge, explaining:

> Typically, plaintiffs who successfully allege that a manufacturer was aware of a defect present a stronger factual basis for their claims than Plaintiffs have here.
>
> * * *
>
> [I]n the case at bar, Plaintiffs' allegations that HP "became familiar with" and was "on notice" of the defect plaguing the Laptops at the time of manufacture and as early as 2002, seem merely conclusory. Plaintiffs make a generalized assertion that the Laptops' alleged "inadequate Design for Reliability" put HP on notice that the Laptops "were and are seriously defective," but reference neither the specific defect alleged in the complaint nor HP's knowledge of that defect. The allegation that HP, as the manufacturer, had

> "access to the aggregate information and data regarding the risk of overheating" is speculative and does not suggest how any tests or information could have alerted HP to the defect.

Wilson v. Hewlett-Packard Co., 668 F.3d 1136, 1146-47 (9th Cir. 2012); *cf. Ahern v. Apple Inc.*, 411 F. Supp. 3d 541, 575-76 (N.D. Cal. 2019) ("Plaintiffs cites [sic] only general allegations in the ACAC that 'Apple did not install any filters for the vents,' that Apple 'acknowledged the Filter Defect exists' in its user manuals, and that Apple '[p]ossessed exclusive knowledge regarding the Filter Defect.' These general and conclusory allegations that Apple owed a duty of disclosure because it was in a superior position to know the facts regarding the alleged defect are not enough. Without 'specific substantiating facts' indicating exclusive knowledge of the Filter Defect, Plaintiffs fail to allege that Apple had a duty to disclose any related information."); *Tietsworth v. Sears*, 720 F. Supp. 2d 1123, 1134 (N.D. Cal. 2010) ("[A] plaintiff cannot establish a duty [to disclose] by pleading, in a purely conclusory fashion, that a defendant was in a superior position to know the truth about a product and actively concealed the defect."); *Sanders v. Apple Inc.*, 672 F. Supp. 2d 978, 986 (N.D. Cal. 2009) (rejecting as too conclusory allegations that Apple "had exclusive knowledge" of the alleged defect, was "in a superior position of knowledge with regard to its own technology," and made representations about the performance of the allegedly defective monitor without disclosing its defect).

Similarly, Plaintiffs allege that how Intel designed its processors equates to a "defect" and that Intel knew that fact. Plaintiffs, however, do not allege any facts to support the conclusory allegations that Intel knew in 2006 it was creating the alleged serious security vulnerabilities discovered in 2017 and later and that Intel chose to do so anyway.[4]

[4] Plaintiffs appear to rely on the technical articles, white papers, product manuals, and patent applications that show the dangers of side-channel attacks to allege Intel's knowledge of

Failure to disclose a defect of which Intel was not aware is not unfair conduct. *See Wilson*, 668 F.3d at 1145 n.5 ("[T]he failure to disclose a fact that a manufacturer does not have a duty to disclose, *i.e.*, a defect of which it is not aware, does not constitute an unfair or fraudulent practice."). Thus, regardless of whether the technical materials disclose Unauthorized Access, Plaintiffs fail to state a claim that Intel engaged in an unfair practice under the UCL based on an omission.

c. Unfair Conduct Absent an Omission

Plaintiffs argue that even without an omission, Intel's conduct was still unfair under the UCL. Plaintiffs assert that Intel "assure[d] buyers of security and performance, and that buyers relied on those assurances." ECF 215 at 30. Plaintiffs also argue the "serial mitigations to address the various exploits" compromised performance and speed, as demonstrated through generic testing of devices and as specifically alleged by some Plaintiffs, contrary to the representations by Intel. There are several flaws with this argument.

The first is that *Plaintiffs*, versus generic "buyers," need to allege that *they* saw or heard representations by Intel and relied on those representations to support the conclusion that Intel's conduct was unfair. This would, however, make Intel's conduct unfair based on fraud from affirmative misrepresentations. Plaintiffs previously and expressly disavowed that they were relying on affirmative misrepresentations for their claims based on fraud. *See Intel II*, 2021 WL 1198299, at *5 n.3. They may not now assert such a claim.

Even if the Court were to consider whether Plaintiffs sufficiently allege misrepresentations by Intel to support that Intel's conduct was unfair based on fraud, Plaintiffs

---

the alleged defects and resulting security vulnerabilities. Those materials, however, also show public disclosure.

do not allege that they heard any *actionable* representation by Intel relating to security, or even performance. Plaintiffs generally allege they heard or read, and relied on, the following representations: (1) Intel's chips were the world's fastest; (2) Intel's chips had advanced performance; (3) Intel was an industry leader in performance and security; (4) Intel's chips had amazing performance that consumers could see and feel; (5) Intel's processors had advanced performance capabilities and were faster; (6) Intel's processors were of superior quality; (7) Intel's processors were the best on the market; (8) computers with Intel processors are high speed and top-of-the-line; and (9) Intel's processors consistently outperformed competitors' processors. The Enterprise Plaintiffs also allege that they relied on "direct and indirect" representations by Intel that its CPUs would provide "superior security, performance, and speed," "would deliver such performance securely," and were fit for use with confidential data. These Plaintiffs do not describe which representations were "indirect" and which were "direct." All Enterprise Plaintiffs make identical boilerplate allegations about the representations on which they allegedly relied.

The Court rejects Plaintiffs' allegations that representations about speed or performance "implicitly" contain a representation related to security and that the chips "would be secure and free from potential exploits." *See Intel II*, 2021 WL 1198299, at *14; c*f. Hauck II*, 816 F. App'x at 43 (affirming dismissal of state consumer protection and unlawful trade practices act claims based on alleged omissions because none "of the alleged statements or omissions [are] 'likely to mislead' consumers 'acting reasonably in the circumstances' to their detriment, given that such consumers would not plausibly believe that AMD's clock-speed representations were premised on any implicit security assurances, or that their devices would be completely impervious to novel cybersecurity threats"). The Court finds that "[t]he representations that the Named

Plaintiffs alleged that they saw or heard are either general statements about speed or performance, which are unrelated to security, are too vague and general to be actionable, or are mere puffery." *Intel II*, 2021 WL 1198299, at *14. The alleged representations on which Plaintiffs allegedly relied do not make Intel's conduct unfair under the UCL.

The next problem is that Plaintiffs do not show how Intel's conduct was unfair based on the alleged defects at the time of the alleged defects—beginning in 2006. All of the conduct on which Plaintiffs base their unfairness argument stems from the mitigation of the exploits, which began in 2018. For example, as of 2015, Plaintiffs who owned devices at that time were receiving the performance they wanted, no one knew about the exploits, and there are no allegations that any Plaintiff's, or other person's, data was breached or compromised. Plaintiffs do not allege how, absent an omission, Intel's conduct was unfair in 2015. This shows that Plaintiffs are really alleging an unfairness claim based on an omission but are trying to argue around it because, as the Court has explained, they cannot state a claim for an omission-based UCL claim. *See Intel II*, 2021 WL 1198299, at *10-11.

Plaintiffs' general factual allegations could be construed as asserting that Intel's conduct was unfair because Intel made design decisions to prioritize speed over security starting in 2006. Plaintiffs, however, repeatedly allege how important speed is to consumers. Absent an omission or Intel's specific knowledge of a security exploit, this general proposition fails to state a claim under the UCL. *See Hauck II*, 816 F. App'x at 43 (rejecting any potential non-fraud based UCL claim because the plaintiffs "have not plausibly alleged that the harm represented by the theoretical risk of a cybersecurity flaw that has not yet been successfully exploited outweighs the other benefits of AMD's processor design").

Plaintiffs also argue that Intel's conduct after learning about Spectre and Meltdown constitutes unfair conduct under the UCL, including by manipulating the embargo period to a longer time than the normal 90 days, advertising the performance and security of products knowing they were uniquely defective and would require extensive mitigation that would affect performance, and charging a premium price during this time. This alleged conduct, however, applies only to persons who purchased or leased products with Intel processors after September 1, 2017, which is 90 days (what Plaintiffs allege is the "normal" embargo period) from June 1, 2017, when Plaintiffs allege Intel learned about Spectre. Thus, this alleged unfair conduct would apply to these Plaintiffs: Carlo Garcia (California), Joseph Phillips (Georgia), Kenneth Woolsey (Idaho), City of New Castle (Pennsylvania), James Bradshaw (Nebraska), Andrew Montoya (New Mexico), and Kathleen Greer (South Carolina).

Intel responds that this conduct is irrelevant because this case is about the alleged defects, not conduct after the security exploits were discovered by Google Project Zero. The Second Amended Complaint, however, contains many allegations relating to Intel's conduct *after* the discovery by Google Project Zero. Intel also argues that Plaintiffs cannot plausibly allege that the discovery of Meltdown and Spectre is material information that would have affected consumers' purchasing decisions because after the public disclosure in 2018, Plaintiffs allege that Intel continued to charge the same premium prices. Thus, contends Intel, based on Plaintiffs' allegations, consumers must not have found the disclosure of Spectre and Meltdown material, and any alleged delay in disclosure could not have mattered. Plaintiffs, however, allege that Intel made public misrepresentations about the effect of Spectre and Meltdown on Intel processors, the fact that Intel's chips were uniquely affected based on its designs, and the effect of the mitigation on performance. Plaintiffs also allege that Intel intentionally suppressed test results

that showed the significant negative effect of the mitigation patches on the performance of Intel processors.

At this stage of the litigation, the Court must accept Plaintiffs' well-pleaded allegations as true. Although Plaintiffs are not alleging a fraud claim based on Intel's alleged misrepresentations, they support Plaintiffs' argument that consumers were not given the full and accurate picture after the public disclosure of Spectre and Meltdown. Thus, at this stage of the proceedings, the Court does not make any inferences about consumer decisions regarding materiality based on the alleged continued consumer purchases and prices charged by Intel. Further, Plaintiffs Garcia, Phillips, Woolsey, Bradshaw, Montoya, Greer, and City of New Castle all allege that had they known about the defects and the effect on performance of the mitigation measures that would be required, they would have made different purchasing decisions.

For this subset of conduct in 2017 and later, the Court considers whether Plaintiffs sufficiently have alleged that Intel's conduct is "immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *McKell*, 142 Cal. App. 4th at 1473. Plaintiffs assert that they have alleged significant injury—the loss of the benefit of their bargain, the vulnerability of their confidential data to a security breach, and the requirement that they download patches that reduce the performance of their CPUs, including freezing, slowed performance, crashing, shutdowns, and termination of programs. Plaintiffs also argue that their injury is not outweighed by any utility because Plaintiffs allege that Intel was motivated by profit, particularly during the latter part of 2017, Intel could have corrected the defects, Intel could have disclosed Spectre and Meltdown sooner, and the CPUs of Intel's competitors are not subject to most of the security exploits.

The balancing test is factually intensive and generally not appropriate to resolve on a motion to dismiss. *See id.* ("[T]he determination whether [a practice] is unfair is one of fact which requires a review of the evidence from both parties. It thus cannot usually be made on demurrer." (citation omitted)). The Ninth Circuit has stated, however, that although it is "mindful that what is 'unfair' is a question of fact, which involves an equitable weighing of all the circumstances, [the Ninth Circuit] will affirm a judgment of dismissal where the complaint fails to allege facts showing that a business practice is unfair." *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1171 (9th Cir. 2012) (simplified). Plaintiffs' Second Amended Complaint fails to allege facts showing that Intel's conduct was unfair, except as to its conduct after Spectre and Meltdown were discovered. Based on Plaintiffs' allegations, it is not clear that Intel had a countervailing business interest other than profit for delaying disclosure for as long as it did (through the holiday season), for downplaying the negative effects of the mitigation, for suppressing the effects of the mitigation, and for continuing to embargo further security exploits that affect only Intel processors. For the seven Plaintiffs who purchased computers after September 1, 2017, they have alleged enough facts at this stage of the proceedings to survive Intel's motion to dismiss on the grounds of failure to state a claim.

2. Nationwide Claim—Quasi-Contract or Unjust Enrichment

A review of California appellate cases shows that a majority of cases accept a claim for unjust enrichment. They note "[t]he elements of a cause of action for unjust enrichment are simply stated as 'receipt of a benefit and unjust retention of the benefit at the expense of another.'" *See, e.g.*, *Prof'l Tax Appeal v. Kennedy-Wilson Holdings, Inc.*, 29 Cal. App. 5th 230, 238 (2018) (quoting *Lectrodryer v. Seoulbank*, 77 Cal. App. 4th 723, 726 (2000)). "The theory of unjust enrichment requires one who acquires a benefit which may not justly be retained, to return either the thing or its equivalent to the aggrieved party so as not to be unjustly enriched."

Otworth v. S. Pac. Transp. Co., 166 Cal. App. 3d 452, 460 (1985). "It is not, strictly speaking, a theory of recovery, 'but an effect: the result of a failure to make restitution under circumstances where it is equitable to do so.'" *Prakashpalan v. Engstrom, Lipscomb & Lack*, 223 Cal. App. 4th 1105, 1132 (2014), *as modified on denial of reh'g* (quoting *Melchior v. New Line Prods., Inc.*, 106 Cal. App. 4th 779, 793 (2003)).

Intel argues that Plaintiffs fail to state a claim for unjust enrichment because without an actionable omission, there is no allegation that Intel retained a benefit that was unjust. As previously discussed, the Court agrees as to all Plaintiffs except the seven Plaintiffs who purchased devices with Intel processors after September 1, 2017. Plaintiffs' allegations that Intel manipulated the embargo period, delayed disclosure to past the holiday season to make more profit, misrepresented that the exploits affected all processors when most of them allegedly only affect Intel's processors, mispresented the negative effects of the mitigation, and intentionally suppressed testing and dissemination of test results of the effects of the mitigation are sufficient at this stage of the litigation plausibly to state a claim that Intel's conduct after the discovery of the exploits resulted in an unjust retention of benefits.

3. Equitable Claims—Adequate Legal Remedy

Intel argues that Plaintiffs' allegation that they may not have an adequate legal remedy is insufficient under *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834 (9th Cir. 2020), and both Plaintiffs' UCL and unjust enrichment claims must be dismissed. In resolving Intel's second motion to dismiss, the Court held that under *Sonner* (then recently decided) Plaintiffs needed to allege, even when pleading in the alternative, that they did not have an adequate remedy at law to request equitable relief. *Intel II*, 2021 WL 1198299, at *11.

Since then, U.S. District Judge Vince Chhabria explained the pleading requirements under *Sonner*:

> *Sonner* primarily speaks to the ability of a federal court to award equitable relief at the end of the case. The ultimate holding of *Sonner* is that a plaintiff "must *establish* that she lacks an adequate remedy at law before *securing*" equitable relief under the UCL and CLRA. 971 F.3d at 844 (emphasis added). While *Sonner* recognized that a complaint seeking equitable relief must "plead 'the basic requisites of the issuance of equitable relief' including 'the inadequacy of remedies at law,'" nothing in *Sonner* precludes plaintiffs from doing so in the alternative to remedies at law. *Id.* at 844 (quoting *O'Shea v. Littleton*, 414 U.S. 488, 502 (1974)). Indeed, the Federal Rules of Civil Procedure permit demands for relief in the alternative. Fed. R. Civ. P. 8(a)(3).
>
> *Sonner*, therefore, should not be understood as a categorical bar to pleading claims for equitable relief under the UCL and damages under the CLRA in a single complaint, as plaintiffs can bring claims in the alternative under different legal theories. For example, a plaintiff may be able to state a claim for equitable relief under the unfair prong of the UCL alongside a claim for damages based on a theory of fraud under the CLRA. *See Elgindy v. AGA Service Company*, 2021 WL 1176535, at *15 (N.D. Cal. Mar. 29, 2021) (declining to dismiss the plaintiffs' claims under the unlawful and unfair prongs of the UCL because only equitable relief was available under this legal theory, despite the availability of a legal remedy for the plaintiffs' claims on a fraud-based theory). The relevant inquiry is not what other claims the plaintiffs have raised, but whether they have plausibly alleged the inadequacy of legal remedies for each claim for equitable relief that they seek.

Cepelak v. HP Inc., 2021 WL 5298022, at *2 (N.D. Cal. Nov. 15, 2021). The Court agrees with Judge Chhabria and, thus, considers whether Plaintiffs have plausibly alleged the inadequacy of legal remedies.

Plaintiffs argue that they have sufficiently alleged the inadequacy of legal remedies for their equitable remedies because they have requested that Intel be prevented from making further misrepresentations about the defects and the security exploits, such as that they affect all processors, and have alleged that going forward they cannot trust Intel's representations about Intel's products. *See id.* at *3 ("Here, the plaintiffs have plausibly alleged the inadequacy of remedies at law with respect to their claims for injunctive relief. . . . The plaintiffs state that,

absent an injunction, they 'will abstain from purchasing [HP printers] even though they would like to do so in the future' because they will not be able to rely on HP's representations (or lack thereof) concerning the alleged defect. This harm cannot be remedied by a future damages action because the plaintiffs cannot bring a lawsuit based on their decision *not* to purchase a printer."). Plaintiffs also argue that the legal remedies are insufficient because they are not as "plain and speedy" as the requested equitable remedies.

"A remedy at law does not exclude one in equity unless it is equally prompt and certain and in other ways efficient." *Am. Life Ins. Co. v. Stewart*, 300 U.S. 203, 214 (1937). Courts have found that the rule set forth in *Stewart* applies when an equitable claim for restitution relies on a different theory than a claim at law that seeks money damages. *See Elgindy v. AGA Serv. Co.*, 2021 WL 1176535, at *15 (N.D. Cal. Mar. 29, 2021) (holding that because the claim for restitution under the UCL was based on a different theory than the plaintiff's legal claims seeking damages, the claim was not barred); *In re JUUL Labs, Inc., Mktg., Sales Practices, & Prod. Liab. Litig.*, 497 F. Supp. 3d 552, 639 (N.D. Cal. 2020) (suggesting that a UCL claim can survive an adequate remedy at law challenge when "the allegations regarding unfair conduct are not otherwise coextensive with plaintiffs' legal claims").

The conduct on which the Court has allowed Plaintiffs' claim of unfair conduct under the UCL and unjust enrichment claims to proceed—Intel's alleged conduct after Google Project Zero discovered the exploits in 2017—is not the same factual conduct on which Plaintiffs based their legal claims. Those claims relied on Intel's conduct before the exploits were discovered, mainly from Intel's design choices in 2006. The equitable claims that the Court is not dismissing also rely extensively on alleged ongoing conduct by Intel, such as manipulating the embargo process and making ongoing misrepresentations about security exploits and their effects as they

continue to be discovered, and the effects of mitigation. Plaintiffs allege this conduct will dissuade them from making future purchases. Such conduct is not amenable to future money damages. *See Cepelak*, 2021 WL 5298022, at *3. Additionally, this conduct makes calculating future money damages difficult. *See IntegrityMessageBoards.com v. Facebook, Inc.*, 2020 WL 6544411, at *7 (N.D. Cal. Nov. 6, 2020) (rejecting a challenge under *Sonner* in part because "plaintiff has no factual basis to quantify its actual damages for future harm"). Further, at this stage in the proceedings, Plaintiffs plausibly have alleged that legal damages may not be as prompt and efficient as equitable restitution. The Court declines to dismiss Plaintiffs' UCL and unjust enrichment claims under *Sonner* at this time.

B. State Subclass Claims

Intel argues that Plaintiffs fail to state a claim under the state subclass claims, which are brought under the consumer protection laws of all states but California, Kentucky, and Massachusetts, plus the District of Columbia. The parties agreed to litigate in the pending motion six bellwether counts under the consumer protection laws of Florida, Illinois, New Jersey, New York, Ohio, and Texas.[5]

[5] Focusing on the bellwether states results in a somewhat awkward analysis because the Court has dismissed the nationwide claims of all Plaintiffs except the seven Plaintiffs who purchased devices after September 1, 2017. These Plaintiffs are from California (no separate state subclass alleged), Georgia, Idaho, Pennsylvania, Nebraska, New Mexico, and South Carolina. Thus, none of them are from the bellwether states. A more efficient analysis at this point would likely be to analyze whether state claims are adequately alleged under the six states for which separate state subclass claims have been raised and the Court has concluded nationwide claims have been sufficiently alleged. The parties, however, only briefed the bellwether states, and there is significant overlap between states. Thus, the Court will analyze the bellwether states as agreed upon by the parties.

1. All Bellwether Deceptive Practices Claims Based on Misrepresentations

In resolving Intel's second motion to dismiss, the Court analyzed Plaintiffs' bellwether claims based on alleged misrepresentations, discussing all the bellwether states' applicable laws and their requirements that a plaintiff be exposed to the alleged misrepresentation (even jurisdictions that do not require reliance). *See Intel II*, 2021 WL 1198299, at *12-14. The Court concluded that "Plaintiffs' allegations about what the Named Plaintiffs from the bellwether jurisdictions allegedly saw and heard are insufficient to support Plaintiffs' alleged deceptive practices claims based on misrepresentations." *Id.* at *14. The Court found the alleged statements to be general statements about speed or performance unrelated to security, statements that were too vague to be actionable, or statements that were mere puffery. *Id.*

The Second Amended Complaint suffers from the same deficiency. As discussed above, the allegations about what every Named Plaintiff saw or heard are still only general statements about speed or performance, statements that are vague, or statements that are mere puffery. They are not actionable as a misrepresentation.

2. All Bellwether Deceptive Practices Claims Based on Omissions

Plaintiffs' state subclass deceptive practices claims based on omissions fail for the same reason the UCL unfairness claim based on an omission fails, even if it did not have other deficiencies. If the technical articles, white papers, product manuals, and patent applications disclose Unauthorized Access, then there is no omission. If those materials do not disclose Unauthorized Access, then Plaintiffs fail sufficiently to allege Intel's knowledge of Unauthorized Access, a required element of an omission claim. Thus, Plaintiffs' fail to state any state claim based on an omission.

3. Unfair Conduct

In Illinois, "to allege that a practice is unfair, a plaintiff must plead that the practice: (1) offends public policy; (2) is immoral, unethical, oppressive, or unscrupulous; and (3) causes substantial injury to consumers." *Aliano v. Ferriss*, 988 N.E.2d 168, 177 (Ill. App. 2013). This is the standard discussed above in analyzing Plaintiffs' nationwide UCL claim, and the outcome is the same for this state subclass claims. Only conduct after September 1, 2017 is actionable.

Ohio applies the Federal Trade Commission (FTC) Act test for such claims. The FTC Act "provides that an 'unfair' practice is one that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'" *Swiger v. Terminix Int'l Co. L.P.*, 1995 WL 396467, at *5 (Ohio Ct. App. June 28, 1995) (quoting 15 U.S.C. § 45(n)); *see also Davis*, 691 F.3d at 1168 (stating that under the FTC Act test "[a] practice is 'unfair' . . . only if it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'" (quoting 15 U.S.C. § 45(n)). Florida also applies this test. *See Porsche Cars N. Am., Inc. v. Diamond*, 140 So. 3d 1090, 1098 (Fla. Dist. Ct. App. 2014) (noting that other cases have applied the FTC's definition from 1964, but holding that because Florida applies the FTC's definition of an unfair practice, the proper definition is the updated one from 1980).

The Court has already found that Plaintiffs have not sufficiently alleged Intel's conduct was unfair for Plaintiffs who purchased or leased products with Intel processors before September 1, 2017. Plaintiffs, however, have sufficiently alleged that Intel's conduct was "unfair" after Google Project Zero discovered the security exploits, for Plaintiffs who purchased products with Intel processors after September 1, 2017. For states applying the FTC test, the Court thus considers whether those Plaintiffs could have reasonably avoided the injury.

"An injury is reasonably avoidable if consumers have reason to anticipate the impending harm and the means to avoid it, or if consumers are aware of, and are reasonably capable of pursuing, potential avenues toward mitigating the injury after the fact." *HSBC Bank*, 691 F.3d at 1168 (quotation marks omitted). Plaintiffs did not have reason to anticipate the impending harm or the means to avoid it. The alleged defects are highly technical, and the average consumer would not comprehend them and would be unable to mitigate them between September 1, 2017 and when the exploits were disclosed in January 2018. Even if a consumer knew to research side-channel attacks and became exposed to the alleged articles and patent applications, they likely would not understand them And, unless they were a highly-skilled computer programmer or hardware engineer, they would be unable to do anything about what they had read. Nor could Plaintiffs avoid the harm of Intel's alleged manipulation of the embargo period or alleged misstatements. The accurate information was in Intel's possession, not the consuming public's.

After both alleged defects became widely known in 2018, average consumers still could do nothing to mitigate them other than download the provided patches. Any degradation in performance or other negative repercussions caused by those patches are beyond the control of the average consumer. As more security exploits of the alleged defects are discovered, the average consumer remains powerless to avoid any potential harm. Additionally, consumers remain unable to mitigate any harm caused by Intel's alleged continuing misstatements. The accurate information about new exploits continues to remain within Intel's knowledge, as does the comprehensive picture about the negative effects of the mitigation efforts. Thus, Plaintiffs could not reasonably have avoided their injuries. The Court dismisses Plaintiffs' claims for

unfair conduct under state law, except for claims based on Intel's alleged conduct after September 1, 2017.

4. Unconscionable Practices

The Court has found no actionable conduct before September 1, 2017. No Plaintiff who bought a product with Intel processors after that date is from any of the bellwether states. The Court therefore will not analyze each bellwether states' law on unconscionability. The Court analyzes Texas law only as a sample bellwether state.

Under the Texas Deceptive Trade Practices Act, an unconscionable action is "an act or practice which, to a consumer's detriment, takes advantage of the lack of knowledge, ability, experience, or capacity of the consumer to a grossly unfair degree." Tex. Bus. & Com Code § 17.45(5).

> When assessing the "unconscionability" of an action, courts look to "what the consumer could have or would have done if he had known about the information," as well as the consumer's relative "knowledge, ability, experience, or capacity." *Peltier Enters., Inc. v. Hilton*, 51 S.W.3d 616, 623 (Tex. App. Ct. 2000). Courts "determine whether the consumer was taken advantage of to a grossly unfair degree by looking at the entire transaction, not just whether a defendant actually intended to take advantage of the consumer." *SCS Builders*, 390 S.W.3d at 541. "To prove an unconscionable action or course of action, a plaintiff must show that the defendant took advantage of his lack of knowledge and the resulting unfairness was glaringly noticeable, flagrant, complete and unmitigated." *Washburn v. Ford*, 521 S.W.3d 871, 877, 2017 WL 2258253, at *5 (Tex. App. May 23, 2017); *see also Parkway Co. v. Woodruff*, 901 S.W.2d 434, 441 (Tex. 1995) ("[U]nconscionability requires that the seller take advantage of special skills and training at the time of the sale.").

In re Gen. Motors LLC Ignition Switch Litig., 257 F. Supp. 3d 372, 449 (S.D.N.Y. 2017), *modified on other grounds on reconsideration*, 2017 WL 3443623 (S.D.N.Y. Aug. 9, 2017). The court in that case concluded that allegations of General Motors' "practice of promoting its vehicles as safe and reliable, despite its knowledge of numerous alleged defects, 'took advantage

of [the plaintiffs'] lack of knowledge' such that 'the resulting unfairness was glaringly noticeable, flagrant, complete and unmitigated.'" *Id.* (quoting Tex. Bus. & Com Code § 17.45(5)).

Here, Plaintiffs allege that after Google Project Zero discovered Spectre and then Meltdown, Intel knew about its processors' unique defects that caused its processors to be susceptible to more exploits than other processors, knew that its processors would require mitigation that would slow down the processors, continued to market its processors as safe and fast, intentionally delayed disclosure of the exploits, including until after the 2017 holiday season, made misrepresentations about the effect of the security exploits and the effect of the mitigation, and actively suppressed testing and public disclosure of the effects of the mitigation. At this stage of the litigation, these allegations are enough to show that Intel took advantage of consumers' lack of knowledge such that the resulting unfairness was glaringly noticeable, flagrant, complete, and unmitigated. Accordingly, at this stage of the proceedings and given the current posture of the motion with the litigation of a bellwether jurisdiction, the Court denies Intel's motion to dismiss Plaintiffs' claim for state law unconscionable practices based on Intel's conduct after September 1, 2017. The Court, however, grants this aspect of Intel's motion to dismiss relating to conduct that occurred before September 1, 2017.

CONCLUSION

The Court GRANTS IN PART Intel's Motion to Dismiss the Second Amended Complaint (ECF 213). The Court dismisses with prejudice all claims except those alleged by Plaintiffs Carlo Garcia, Joseph Phillips, Kenneth Woolsey, City of New Castle, James Bradshaw, Andrew Montoya, and Kathleen Greer for alleged conduct by Intel occurring on or after September 1, 2017. The Court also dismisses the claims of these seven Plaintiffs other than: (a) their nationwide claim under California's Unfair Competition Law alleging unfair conduct;

(b) their nationwide claim alleging unjust enrichment; (c) their state subclass claim alleging unfair conduct; and (d) their state subclass claim alleging unconscionable conduct. In short, the Court dismisses with prejudice all claims based on Intel's alleged conduct occurring *before* September 1, 2017. The Court directs the Clerk of the Court to send a copy of this Opinion and Order to the Clerk of the Judicial Panel on Multidistrict Litigation.

IT IS SO ORDERED.

DATED this 26th day of January, 2022.

/s/ *Michael H. Simon*
Michael H. Simon
United States District Judge